FSA's Proposed Numbering System for IT Security Findings

Keeping track of IT security findings is a challenge. This challenge is due to a number of reasons, including the following:

- Findings are generated from multiple sources—and sometimes the same finding is reported by multiple sources
- Within each finding source (eg, IG, risk assessment, C&A), there are often several iterations of findings reports—eg preliminary reports, interim reports, and final reports
- It is not always clear what, exactly, the security finding is (you often have to "read between the lines" to extract the actual finding)
- There are multiple tracking systems for findings, each of which may state the finding in a slightly different way
- What, exactly, *is* a finding? Any potential vulnerability or weakness noted by any auditor? Just those reported vulnerabilities/weaknesses that will be addressed in a formal POA&M? Just those that must be reported to OMB?

Last—but certainly not least—there is no standardized method of numbering/labeling findings. This paper outlines a proposed methodology for such a standardized numbering system, as well as the steps and key factors necessary to ensure that any such numbering system will be successful.

Note: A numbering system will only be as effective as the overall environment in which that numbering system exists. A numbering system is not a replacement for an orderly process for discovering, documenting, and tracking the status of security findings.

Key Factors for Success

- ED OCIO, working closely with FSA CIO, should establish more "front-end" control over what happens to findings when they are first "discovered." Such front-end control is critical to effectively implementing a standardized numbering system for IT security findings.
- OCIO should establish a clear reporting chain for documenting and tracking findings, from the top down.
- IG should phrase findings in more concrete language, and make its reporting requirements clear.
- OCIO should consider centralized control of findings. (For example, all findings, from all sources, for all systems, must first go the OCIO, which will then number the findings, enter them in the PIP Portal, and distribute them to the affected security personnel.)
- OCIO/FSA should determine how the PIP Portal will relate to the existing IG tracking system (ARTS)

- If centralized control is not an option, then OCIO and FSA should establish mechanisms for coordination among offices.
- The numbering scheme will be part of a database system that will allow findings to be sorted by a variety of categories (eg, sort by source, sort by criticality, sort by status)
- OCIO and FSA CIO should consider integrating existing finding tracking systems into one centralized repository—eg, the Performance Improvement Portal.

Preliminary Steps

- Identify ALL finding sources
- Identify all current numbering systems, if any
- Conduct a focus group with affected personnel to solicit input on how to improve the finding tracking process, and to solicit input on elements of the new numbering system
- Identify all current finding tracking systems (database, CAPs, POAMs, ARTS, etc.)—and determine if they have numbering systems
- Identify any current requirements for reporting that may include a numbering scheme (eg, OMB requirements)
- Determine any limits on numbering scheme (eg, if the PIP is limited to a certain number of characters)
- Diagram the "As Is" state of the finding tracking process
- Diagram a "Future State" diagram of the finding tracking process
- Create an Implementation Plan to move from As Is to Future State

Possible Numbering Schemes

By system
By office
By finding source
By date
By type of finding (management, operational, technical, administrative)
By priority (high, medium, low)
By resources required to remediate
By concur/nonconcur/false positive status
By program office
By business line

Examples: